

Practice-oriented provable security

The case of pairing based cryptographic schemes

David Galindo

`d.galindo@cs.ru.nl`

Security of Systems

Department of Computer Science

Radboud Universiteit Nijmegen

Pairings in Cryptography Workshop, DCU

June 14

Outline

- Exact security preliminaries
 - Non-tight reductions & key sizes
 - Negative examples: larger keys

Outline

- Exact security preliminaries
 - Non-tight reductions & key sizes
 - Negative examples: larger keys
- **Boneh&Lynn&Shacham short signature scheme**
 - Katz&Wang modification
 - New interpretation/problems/assumptions
 - Comparison with q -BDH problems

Outline

- Exact security preliminaries
 - Non-tight reductions & key sizes
 - Negative examples: larger keys
- **Boneh&Lynn&Shacham short signature scheme**
 - Katz&Wang modification
 - New interpretation/problems/assumptions
 - Comparison with q -BDH problems
- **Boneh&Franklin IBE scheme**
 - A tight reduction under a new assumption

Outline

- Exact security preliminaries
 - Non-tight reductions & key sizes
 - Negative examples: larger keys
- **Boneh&Lynn&Shacham short signature scheme**
 - Katz&Wang modification
 - New interpretation/problems/assumptions
 - Comparison with q -BDH problems
- **Boneh&Franklin IBE scheme**
 - A tight reduction under a new assumption
- Conclusions & Open Problems

Introduction

- Provable security
 - Security definition
 - Hard problem
- } Polynomial reduction

Introduction

- Provable security

Security definition

Hard problem

} Polynomial reduction

Asymptotical equivalences

Introduction

- Provable security
 - Security definition
 - Hard problem } Polynomial reduction

Asymptotical equivalences

- Practice-oriented provable security (exact security)
 - Quantifying security { Exact reductions
Security parameters

Introduction

- Provable security
 - Security definition
 - Hard problem } Polynomial reduction

Asymptotical equivalences

- Practice-oriented provable security (exact security)
 - Quantifying security { Exact reductions
Security parameters

Practical equivalences

Goal: Efficient schemes & Trusted assumptions

Concrete security (I)

Security level A problem \mathcal{P} is said to have security level 2^t when the minimal computational effort to solve this problem should be of the order of 2^t 3-DES encryptions.

Concrete security (I)

Security level A problem \mathcal{P} is said to have security level 2^t when the minimal computational effort to solve this problem should be of the order of 2^t 3-DES encryptions.

Currently, it is required $t \geq 80$. It is often assumed that

$$q_S, q_D, q_E \leq 2^{30} \text{ and } q_{\text{RO}} \leq 2^{60}$$

Concrete security (I)

Security level A problem \mathcal{P} is said to have security level 2^t when the minimal computational effort to solve this problem should be of the order of 2^t 3-DES encryptions.

Currently, it is required $t \geq 80$. It is often assumed that

$$q_S, q_D, q_E \leq 2^{30} \text{ and } q_{\text{RO}} \leq 2^{60}$$

Practical computational complexity \mathcal{P}_1 and \mathcal{P}_2 are assumed to have similar complexity in practice when

Concrete security (I)

Security level A problem \mathcal{P} is said to have security level 2^t when the minimal computational effort to solve this problem should be of the order of 2^t 3-DES encryptions.

Currently, it is required $t \geq 80$. It is often assumed that

$$q_S, q_D, q_E \leq 2^{30} \text{ and } q_{\text{RO}} \leq 2^{60}$$

Practical computational complexity \mathcal{P}_1 and \mathcal{P}_2 are assumed to have similar complexity in practice when

1. There exists a reduction from \mathcal{P}_2 to \mathcal{P}_1

Concrete security (I)

Security level A problem \mathcal{P} is said to have security level 2^t when the minimal computational effort to solve this problem should be of the order of 2^t 3-DES encryptions.

Currently, it is required $t \geq 80$. It is often assumed that

$$q_S, q_D, q_E \leq 2^{30} \text{ and } q_{\text{RO}} \leq 2^{60}$$

Practical computational complexity \mathcal{P}_1 and \mathcal{P}_2 are assumed to have similar complexity in practice when

1. There exists a reduction from \mathcal{P}_2 to \mathcal{P}_1
2. We only know to solve \mathcal{P}_2 by solving \mathcal{P}_1

Concrete security (I)

Security level A problem \mathcal{P} is said to have security level 2^t when the minimal computational effort to solve this problem should be of the order of 2^t 3-DES encryptions.

Currently, it is required $t \geq 80$. It is often assumed that $q_S, q_D, q_E \leq 2^{30}$ and $q_{\text{RO}} \leq 2^{60}$

Practical computational complexity \mathcal{P}_1 and \mathcal{P}_2 are assumed to have similar complexity in practice when

1. There exists a reduction from \mathcal{P}_2 to \mathcal{P}_1
2. We only know to solve \mathcal{P}_2 by solving \mathcal{P}_1

For instance, **CDH** and **DDH**; **factoring** and **QR**

Concrete security (I)

Security level A problem \mathcal{P} is said to have security level 2^t when the minimal computational effort to solve this problem should be of the order of 2^t 3-DES encryptions.

Currently, it is required $t \geq 80$. It is often assumed that $q_S, q_D, q_E \leq 2^{30}$ and $q_{\text{RO}} \leq 2^{60}$

Practical computational complexity \mathcal{P}_1 and \mathcal{P}_2 are assumed to have similar complexity in practice when

1. There exists a reduction from \mathcal{P}_2 to \mathcal{P}_1
2. We only know to solve \mathcal{P}_2 by solving \mathcal{P}_1

For instance, CDH and DDH; factoring and QR

DL^{ec} and BDH; DL^{ff} and BDH; BDH and BDDH

Concrete security (II)

Scheme challenger

\mathcal{P} challenger

Scheme adversary \mathcal{A}

$(t, q_{\mathcal{O}_i}, \varepsilon)$

\mathcal{P} solver \mathcal{B}

(t', ε')

Concrete security (II)

Scheme challenger

\mathcal{P} challenger

Scheme adversary \mathcal{A}

$(t, q_{\mathcal{O}_i}, \varepsilon)$

\mathcal{P} solver \mathcal{B}

(t', ε')

Security reductions are said to be:

• **tight** if $\frac{t'}{\varepsilon'} \approx \frac{t}{\varepsilon}$

Concrete security (II)

Scheme challenger

\mathcal{P} challenger

Scheme adversary \mathcal{A}

$(t, q_{\mathcal{O}_i}, \varepsilon)$

\mathcal{P} solver \mathcal{B}

(t', ε')

Security reductions are said to be:

- **tight** if $\frac{t'}{\varepsilon'} \approx \frac{t}{\varepsilon}$
- **non-tight** if $\frac{t'}{\varepsilon'} \geq q_{\mathcal{O}_i} \frac{t}{\varepsilon}$

Concrete security (II)

Scheme challenger

\mathcal{P} challenger

Scheme adversary \mathcal{A}

$(t, q_{\mathcal{O}_i}, \varepsilon)$

\mathcal{P} solver \mathcal{B}

(t', ε')

Security reductions are said to be:

- **tight** if $\frac{t'}{\varepsilon'} \approx \frac{t}{\varepsilon}$
- **non-tight** if $\frac{t'}{\varepsilon'} \geq q_{\mathcal{O}_i} \frac{t}{\varepsilon}$

Non-tightness means **slower protocols**

The problem

If we take a look at protocols using bilinear groups and maps

The problem

If we take a look at protocols using bilinear groups and maps

- Proofs are usually **non-tight**

The problem

If we take a look at protocols using bilinear groups and maps

- Proofs are usually **non-tight**
 - This means slower protocols (exact security approach), but...

The problem

If we take a look at protocols using bilinear groups and maps

- Proofs are usually **non-tight**
 - This means slower protocols (exact security approach), but...
 - This is **overlooked**, or
 - **Security parameters are proposed as if the reductions were tight!**

The problem

If we take a look at protocols using bilinear groups and maps

- Proofs are usually **non-tight**
 - This means slower protocols (exact security approach), but...
 - This is **overlooked**, or
 - **Security parameters are proposed as if the reductions were tight!**
- Our goals:
 - Compute key sizes related to security reductions (**negative results**)
 - Solve these problems inside the exact security approach

Pairings main parameters

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T.$$

Using elliptic curves

Pairings main parameters

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T.$$

Using elliptic curves

- **Supersingular case:**

$$\mathbb{G}_1 = \mathbb{G}_2 \subseteq E(\mathbb{F}_q); \quad \mathbb{G}_T \subseteq \mathbb{F}_{q^k}; \quad k \leq 6$$

$$k = 4, 6 \Rightarrow \mathbb{F}_q \text{ has characteristic } 2 \text{ or } 3$$

Pairings main parameters

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T.$$

Using elliptic curves

- **Supersingular case:**

$$\mathbb{G}_1 = \mathbb{G}_2 \subseteq E(\mathbb{F}_q); \quad \mathbb{G}_T \subseteq \mathbb{F}_{q^k}; \quad k \leq 6$$

$k = 4, 6 \Rightarrow \mathbb{F}_q$ has characteristic 2 or 3

- **Ordinary case:**

$$\mathbb{G}_1 \subseteq E(\mathbb{F}_q); \quad \mathbb{G}_2 \subseteq E(\mathbb{F}_{q^{k/2}}); \quad \mathbb{G}_T \subseteq \mathbb{F}_{q^k}$$

Pairings main parameters

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T.$$

Using elliptic curves

- **Supersingular case:**

$$\mathbb{G}_1 = \mathbb{G}_2 \subseteq E(\mathbb{F}_q); \quad \mathbb{G}_T \subseteq \mathbb{F}_{q^k}; \quad k \leq 6$$

$k = 4, 6 \Rightarrow \mathbb{F}_q$ has characteristic 2 or 3

- **Ordinary case:**

$$\mathbb{G}_1 \subseteq E(\mathbb{F}_q); \quad \mathbb{G}_2 \subseteq E(\mathbb{F}_{q^{k/2}}); \quad \mathbb{G}_T \subseteq \mathbb{F}_{q^k}$$

Main parameters: $p := \#\mathbb{G}_1$ k $|q|$ $|q^k|$

Key Sizes (I)

BLS signature scheme $\epsilon' \approx \frac{\epsilon}{q_S}$

Key Sizes (I)

BLS signature scheme $\varepsilon' \approx \frac{\varepsilon}{q_S}$

$$k = 6 \quad |p| \approx 207, |q| \approx 356$$

$$k = 10 \quad |p| \approx 210, |q| \approx 263$$

(240 bits DSA signatures)

Key Sizes (I)

BLS signature scheme $\epsilon' \approx \frac{\epsilon}{q_S}$

$$k = 6 \quad |p| \approx 207, |q| \approx 356$$

$$k = 10 \quad |p| \approx 210, |q| \approx 263$$

(240 bits DSA signatures)

IND-ID-CPA Waters's scheme $\epsilon' \approx \frac{\epsilon}{2^{13}q_E}$

Key Sizes (I)

BLS signature scheme $\epsilon' \approx \frac{\epsilon}{q_S}$

$$k = 6 \quad |p| \approx 207, |q| \approx 356$$

$$k = 10 \quad |p| \approx 210, |q| \approx 263$$

(240 bits DSA signatures)

IND-ID-CPA Waters's scheme $\epsilon' \approx \frac{\epsilon}{2^{13}q_E}$

SS	k	$ p $	$ q $	$ q^k $	EGff	EGcc
Yes	2	219	1292	2584	34	129
Yes	6	223	748	4483	22	85
No	6	229	458	2584	7	27
No	10	229	287	2870	6	23

Key Sizes (II)

IND-ID-CPA Boneh-Boyen scheme $\varepsilon' \approx \frac{\varepsilon}{q_H}$

Key Sizes (II)

IND-ID-CPA Boneh-Boyen scheme $\varepsilon' \approx \frac{\varepsilon}{q_H}$

SS	k	$ p $	$ q $	$ q^k $	EGff	EGcc
Yes	6	261	1058	6347	47	179
No	6	304	607	3640	18	69
No	12	267	334	4000	14	51

Key Sizes (II)

IND-ID-CPA Boneh-Boyen scheme $\epsilon' \approx \frac{\epsilon}{q_H}$

	SS	k	$ p $	$ q $	$ q^k $	EGff	EGcc
	Yes	6	261	1058	6347	47	179
	No	6	304	607	3640	18	69
	No	12	267	334	4000	14	51
2^{-240}	No	20	453	633	12650	204	782

Key Sizes (III)

IND-ID-CPA Boneh-Franklin scheme $\epsilon' \approx \frac{\epsilon}{q_D q_H}$

Key Sizes (III)

IND-ID-CPA Boneh-Franklin scheme $\varepsilon' \approx \frac{\varepsilon}{q_D q_H}$

SS	k	$ p $	$ q $	$ q^k $	EGff	EGcc
No	10	324	648	5657	147	561
No	20	328	354	5657	31	117

Key Sizes (III)

IND-ID-CPA Boneh-Franklin scheme $\varepsilon' \approx \frac{\varepsilon}{q_D q_H}$

SS	k	$ p $	$ q $	$ q^k $	EGff	EGcc
No	10	324	648	5657	147	561
No	20	328	354	5657	31	117

IND-ID-CPA HIBE's $\varepsilon' \approx \frac{\varepsilon}{q_E^t}$, toy example $t = 10$

Key Sizes (III)

IND-ID-CPA Boneh-Franklin scheme $\varepsilon' \approx \frac{\varepsilon}{q_D q_H}$

SS	k	$ p $	$ q $	$ q^k $	EGff	EGcc
No	10	324	648	5657	147	561
No	20	328	354	5657	31	117

IND-ID-CPA HIBE's $\varepsilon' \approx \frac{\varepsilon}{q_E^t}$, toy example $t = 10$

SS	k	$ p $	$ q $	$ q^k $	EGff	EGcc
No	20	580	1079	21567	975	3734

BLS signature scheme: Description

Let $(\mathbb{G}_1, \mathbb{G}_2)$ a bilinear group pair with $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$,
 $H : \{0, 1\}^* \rightarrow \mathbb{G}_1$ and $\mathbb{G}_2 = \langle P_2 \rangle$.

BLS signature scheme: Description

Let $(\mathbb{G}_1, \mathbb{G}_2)$ a bilinear group pair with $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$,
 $H : \{0, 1\}^* \rightarrow \mathbb{G}_1$ and $\mathbb{G}_2 = \langle P_2 \rangle$.

KeyGeneration Pick random $x \leftarrow \mathbb{Z}_p^*$ and compute $V = xP_2$.
The public key is $V \in \mathbb{G}_2$. The private key is x .

BLS signature scheme: Description

Let $(\mathbb{G}_1, \mathbb{G}_2)$ a bilinear group pair with $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$,
 $H : \{0, 1\}^* \rightarrow \mathbb{G}_1$ and $\mathbb{G}_2 = \langle P_2 \rangle$.

KeyGeneration Pick random $x \leftarrow \mathbb{Z}_p^*$ and compute $V = xP_2$.
The public key is $V \in \mathbb{G}_2$. The private key is x .

Signing Given a private key $x \in \mathbb{Z}_p^*$, and a message
 $M \in \{0, 1\}^*$, compute $Q = H(M) \in \mathbb{G}_1$ and $\sigma = xQ$. The
signature is $\sigma \in \mathbb{G}_1$.

BLS signature scheme: Description

Let $(\mathbb{G}_1, \mathbb{G}_2)$ a bilinear group pair with $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, $H : \{0, 1\}^* \rightarrow \mathbb{G}_1$ and $\mathbb{G}_2 = \langle P_2 \rangle$.

KeyGeneration Pick random $x \leftarrow \mathbb{Z}_p^*$ and compute $V = xP_2$.
The public key is $V \in \mathbb{G}_2$. The private key is x .

Signing Given a private key $x \in \mathbb{Z}_p^*$, and a message $M \in \{0, 1\}^*$, compute $Q = H(M) \in \mathbb{G}_1$ and $\sigma = xQ$. The signature is $\sigma \in \mathbb{G}_1$.

Verification Given $(V, M, \sigma) \in \mathbb{G}_2 \times \{0, 1\}^* \times \mathbb{G}_1$, compute $Q = H(M) \in \mathbb{G}_1$ and check if $\hat{e}(Q, V) = \hat{e}(\sigma, P_2)$. If so, output `valid`; otherwise output `invalid`.

BLS exact security

Result Let $(\mathbb{G}_1, \mathbb{G}_2)$ a (t', ε') -bilinear group pair of order p . Then the signature scheme on $(\mathbb{G}_1, \mathbb{G}_2)$ is $(t, q_S, q_H, \varepsilon)$ -secure against existential forgery under and adaptive chosen message attack (in the random oracle model), for all t and ε satisfying

$$t \leq t' - c_{\mathbb{G}_1}(q_H + 2q_S) \quad \text{and} \quad \boxed{\varepsilon \geq e(q_S + 1) \cdot \varepsilon'}$$

Here $c_{\mathbb{G}_1}$ is the time for computing an exponentiation in \mathbb{G}_1 and e is the base of the natural logarithm.

Modification by Katz&Wang'03

Modification by Katz&Wang'03

The global parameters are the same as in BLS scheme, except for a new hash function $G : \{0, 1\}^* \rightarrow \{0, 1\}$.

Modification by Katz&Wang'03

The global parameters are the same as in BLS scheme, except for a new hash function $G : \{0, 1\}^* \rightarrow \{0, 1\}$.

NewKeyGeneration The same as **KeyGeneration** in BLS scheme. The public key is $V \in \mathbb{G}_2$. The private key is $x \in \mathbb{Z}_p^*$.

Modification by Katz&Wang'03

The global parameters are the same as in BLS scheme, except for a new hash function $G : \{0, 1\}^* \rightarrow \{0, 1\}$.

NewKeyGeneration The same as **KeyGeneration** in BLS scheme. The public key is $V \in \mathbb{G}_2$. The private key is $x \in \mathbb{Z}_p^*$.

NewSigning Given a private key $x \in \mathbb{Z}_p^*$, and a message $M \in \{0, 1\}^*$, compute $b = G(x, M)$, $Q = H(b, M) \in \mathbb{G}_1$ and $\sigma = xQ$. The signature is $(b, \sigma) \in \{0, 1\} \times \mathbb{G}_1$.

Modification by Katz&Wang'03

The global parameters are the same as in BLS scheme, except for a new hash function $G : \{0, 1\}^* \rightarrow \{0, 1\}$.

NewKeyGeneration The same as **KeyGeneration** in BLS scheme. The public key is $V \in \mathbb{G}_2$. The private key is $x \in \mathbb{Z}_p^*$.

NewSigning Given a private key $x \in \mathbb{Z}_p^*$, and a message $M \in \{0, 1\}^*$, compute $b = G(x, M)$, $Q = H(b, M) \in \mathbb{G}_1$ and $\sigma = xQ$. The signature is $(b, \sigma) \in \{0, 1\} \times \mathbb{G}_1$.

NewVerification Given $(V, M, b, \sigma) \in \mathbb{G}_2 \times \{0, 1\}^* \times \{0, 1\} \times \mathbb{G}_1$, compute $Q = H(b, M) \in \mathbb{G}_1$ and check if $\hat{e}(Q, V) = \hat{e}(\sigma, P_2)$. If so, output `valid`; otherwise output `invalid`.

ModifiedBLS exact security

Result Let $(\mathbb{G}_1, \mathbb{G}_2)$ a (t', ε') -bilinear group pair of order p . Then the signature scheme on $(\mathbb{G}_1, \mathbb{G}_2)$ is $(t, \varepsilon, q_S, q_H, \varepsilon)$ -secure against existential forgery under and adaptive chosen message attack (in the random oracle model), for all t and ε satisfying

$$t \leq t' - c_{\mathbb{G}_1}(q_H + 2q_S) \quad \text{and} \quad \boxed{\varepsilon \geq 2 \cdot \varepsilon'}$$

ModifiedBLS exact security

Result Let $(\mathbb{G}_1, \mathbb{G}_2)$ a (t', ε') -bilinear group pair of order p . Then the signature scheme on $(\mathbb{G}_1, \mathbb{G}_2)$ is $(t, \varepsilon, q_S, q_H, \varepsilon)$ -secure against existential forgery under and adaptive chosen message attack (in the random oracle model), for all t and ε satisfying

$$t \leq t' - c_{\mathbb{G}_1}(q_H + 2q_S) \quad \text{and} \quad \boxed{\varepsilon \geq 2 \cdot \varepsilon'}$$

Now the exact security analysis leads to

$|p| \geq 150$ and $|q| \geq 209$ (optimistically $|q| \geq 189$) then **short signatures**

Interpretations for Katz&Wang

(At least) Two possibilities:

Interpretations for Katz&Wang

(At least) Two possibilities:

- 1 Yet another anomaly of Random Oracles

Adding 1 bit to the RO results in a tight reduction?... come on!

Interpretations for Katz&Wang

(At least) Two possibilities:

1 Yet another anomaly of Random Oracles

Adding 1 bit to the RO results in a tight reduction?... come on!

Implication: don't take into account RO exact security,
i.e. easier cryptographer's task :-)

Interpretations for Katz&Wang

(At least) Two possibilities:

1 Yet another anomaly of Random Oracles

Adding 1 bit to the RO results in a tight reduction?... come on!

Implication: don't take into account RO exact security, i.e. easier cryptographer's task :-)

2 Menezes&Koblitz discussion on FDH-RSA

New problems: CDH1 and CDH2

CDH1 ($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) .

New problems: CDH1 and CDH2

CDH1 ($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,

New problems: CDH1 and CDH2

CDH1 ($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,
- aP , where $a \leftarrow \mathbb{Z}_p^*$ is unknown;

New problems: CDH1 and CDH2

CDH1 ($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,
- aP , where $a \leftarrow \mathbb{Z}_p^*$ is unknown;
- a set $Q_{\text{set}} = \{Q_1, \dots, Q_{q_S+q_H}\}$ of uniformly independent random elements from \mathbb{G} ;

New problems: CDH1 and CDH2

CDH1 ($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,
- aP , where $a \leftarrow \mathbb{Z}_p^*$ is unknown;
- a set $Q_{\text{set}} = \{Q_1, \dots, Q_{q_S+q_H}\}$ of uniformly independent random elements from \mathbb{G} ;
- You can adaptively select up to q_S of those Q_i , and you'll be given the solutions aQ_i .

New problems: CDH1 and CDH2

CDH1 ($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,
- aP , where $a \leftarrow \mathbb{Z}_p^*$ is unknown;
- a set $Q_{\text{set}} = \{Q_1, \dots, Q_{q_S+q_H}\}$ of uniformly independent random elements from \mathbb{G} ;
- You can adaptively select up to q_S of those Q_i , and you'll be given the solutions aQ_i .

You must produce a solution $aQ_j \in \mathbb{G}$ for one of the remaining Q_j .

New problems: CDH1 and CDH2

CDH2($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) .

New problems: CDH1 and CDH2

CDH2($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,

New problems: CDH1 and CDH2

CDH2($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,
- aP , where $a \leftarrow \mathbb{Z}_p^*$ is unknown;

New problems: CDH1 and CDH2

CDH2($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,
- aP , where $a \leftarrow \mathbb{Z}_p^*$ is unknown;
- a set $Q_{\text{set}} = \{(Q_1, R_1), \dots, (Q_{q_S+q_H}, R_{q_S+q_H})\}$ of uniformly independent random pair elements from \mathbb{G} ;

New problems: CDH1 and CDH2

CDH2($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,
- aP , where $a \leftarrow \mathbb{Z}_p^*$ is unknown;
- a set $Q_{\text{set}} = \{(Q_1, R_1), \dots, (Q_{q_S+q_H}, R_{q_S+q_H})\}$ of uniformly independent random pair elements from \mathbb{G} ;
- You can adaptively select up to q_S of those pairs, and you'll be given the a -multiple of exactly one (randomly selected) element of the pair

New problems: CDH1 and CDH2

CDH2($q_S, q_H + q_S$) problem on (\mathbb{G}, \mathbb{G}) . Given

- A bilinear group pair (\mathbb{G}, \mathbb{G}) , with $\mathbb{G} = \langle P \rangle$,
- aP , where $a \leftarrow \mathbb{Z}_p^*$ is unknown;
- a set $Q_{\text{set}} = \{(Q_1, R_1), \dots, (Q_{q_S+q_H}, R_{q_S+q_H})\}$ of uniformly independent random pair elements from \mathbb{G} ;
- You can adaptively select up to q_S of those pairs, and you'll be given the a -multiple of exactly one (randomly selected) element of the pair

You must produce the a -multiple of either element of the remaining pairs.

Schemes versus Problems

Result 1. The security of BLS scheme is **tightly** equivalent to the hardness of $\text{CDH1}(q_S, q_S + q_H)$ problem.

Schemes versus Problems

Result 1. The security of BLS scheme is **tightly** equivalent to the hardness of $\text{CDH1}(q_S, q_S + q_H)$ problem.

Result 2. The security of KW modification is **tightly** equivalent to the hardness of $\text{CDH2}(q_S, q_S + q_H)$ problem.

Schemes versus Problems

Result 1. The security of BLS scheme is **tightly** equivalent to the hardness of $\text{CDH1}(q_S, q_S + q_H)$ problem.

Result 2. The security of KW modification is **tightly** equivalent to the hardness of $\text{CDH2}(q_S, q_S + q_H)$ problem.

Result 3 (KW). $\text{CDH2}(q_S, q_S + q_H)$ and CDH problems are **tightly** equivalent

Schemes versus Problems

Result 1. The security of BLS scheme is **tightly** equivalent to the hardness of $\text{CDH1}(q_S, q_S + q_H)$ problem.

Result 2. The security of KW modification is **tightly** equivalent to the hardness of $\text{CDH2}(q_S, q_S + q_H)$ problem.

Result 3 (KW). $\text{CDH2}(q_S, q_S + q_H)$ and CDH problems are **tightly** equivalent

Result 4 (BLS). $\text{CDH1}(q_S, q_S + q_H)$ and CDH problems are equivalent, but **not tightly** equivalent

Schemes versus Problems

Result 1. The security of BLS scheme is **tightly** equivalent to the hardness of $\text{CDH1}(q_S, q_S + q_H)$ problem.

Result 2. The security of KW modification is **tightly** equivalent to the hardness of $\text{CDH2}(q_S, q_S + q_H)$ problem.

Result 3 (KW). $\text{CDH2}(q_S, q_S + q_H)$ and CDH problems are **tightly** equivalent

Result 4 (BLS). $\text{CDH1}(q_S, q_S + q_H)$ and CDH problems are equivalent, but **not tightly** equivalent

However, that CDH1 could be easier to solve than CDH2 defies common sense.

Practical CDH1 assumption

The problems CDH and $\text{CDH1}(q_S, q_S + q_H)$ have similar computational complexity \Rightarrow **short signatures**

Practical CDH1 assumption

The problems CDH and $\text{CDH1}(q_S, q_S + q_H)$ have similar computational complexity \Rightarrow **short signatures**

Rationale:

- It satisfies all traditional previous requirements.

Practical CDH1 assumption

The problems CDH and $\text{CDH1}(q_S, q_S + q_H)$ have similar computational complexity \Rightarrow **short signatures**

Rationale:

- It satisfies all traditional previous requirements.
- More robust practical assumption than q -BDH practical assumptions.

Practical CDH1 assumption

The problems CDH and CDH1 ($q_S, q_S + q_H$) have similar computational complexity \Rightarrow **short signatures**

Rationale:

- It satisfies all traditional previous requirements.
- More robust practical assumption than q -BDH practical assumptions.
- CDH2 is actually equivalent to CDH.

Practical CDH1 assumption

The problems CDH and CDH1 ($q_S, q_S + q_H$) have similar computational complexity \Rightarrow **short signatures**

Rationale:

- It satisfies all traditional previous requirements.
- More robust practical assumption than q -BDH practical assumptions.
- CDH2 is actually equivalent to CDH.

Interpretation: KW result does not point out a deficiency of the RO but **an inherent limitation of black-box reductions.**

Final remarks

Step 1 Provide a provably secure protocol satisfying a new functionality

Final remarks

Step 1 Provide a provably secure protocol satisfying a new functionality

Step 2 Look for tight security reductions

- Deeper understanding of the design
- Improvements on efficiency
- Discovery of new strategies, deficiencies...

Final remarks

Step 1 Provide a provably secure protocol satisfying a new functionality

Step 2 Look for tight security reductions

- Deeper understanding of the design
- Improvements on efficiency
- Discovery of new strategies, deficiencies...

That's all!